



## Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at <http://about.jstor.org/participate-jstor/individuals/early-journal-content>.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact [support@jstor.org](mailto:support@jstor.org).

# EXAMPLES OF NORMAL DOMAINS OF RATIONALITY BELONGING TO ELEMENTARY GROUPS.

BY G. A. MILLER.

## Introduction.

The object of the present expository article is to furnish an approach, which is very direct and elementary from a certain point of view, for a study of the theory of groups of normal domains of rationality. Only a few fundamental theorems relating to the theories of groups and domains of rationality will be assumed as known. The most important of these theorems for our purpose may be stated as follows: If the irrational number  $\rho_1$  generates a normal domain and if the other roots ( $\rho_2, \rho_3, \dots, \rho_n$ ) of the irreducible equation which  $\rho_1$  satisfies are expressed as rational functions of  $\rho_1$  then we can obtain the group of this domain as a regular substitution group by replacing  $\rho_1$  successively by  $\rho_1, \rho_2, \dots, \rho_n$  in all these rational functions and by noting the permutations of the values of these functions.\*

It will always be assumed, in what follows, that the irreducible equation  $f(x) = 0$  which  $\rho_1$  satisfies, has rational coefficients and hence it lies in the natural or absolute domain of rationality. Hence, we shall assume that  $f(x)$  is not the product of two rational integral functions of  $x$  with rational coefficients. In the first section of the present article we shall determine a domain of rationality for each one of the groups whose order is less than 8. Only one of these groups is non-abelian, viz., the symmetric group of order 6. In the second section we shall consider briefly domains belonging to two infinite systems of very elementary groups. The central point of view will be the group and its applications rather than the domain and its properties.

### 1. Domains Belonging to the Groups whose Orders are less than 8.

In case of the group of order 2 the considerations are very elementary and may appear trivial. For the sake of completeness from the present point of view we shall, however, give some of the details even in this case. The two roots of any quadratic equation  $ax^2 + bx + c = 0$  are rational functions of each other since the sum of these roots is  $-b/a$ . If  $\rho_1, \rho_2$  are these roots it results that  $\rho_1 = \varphi_1(\rho_1) = \rho_1, \rho_2 = \varphi_2(\rho_1) = -b/a - \rho_1$ . By replacing  $\rho_1$  in these functions successively by  $\rho_1$  and  $\rho_2$ , and noting the

---

\* Cf. H. Weber, *Kleines Lehrbuch der Algebra*, 1912, p. 245; F. Cajori, *Theory of Equations*, 1912, p. 161.

permutations of these values, we obtain the following two substitutions: 1,  $(\rho_1\rho_2)$ . Hence each root of any irreducible quadratic equation generates a normal domain which belongs to the group of order 2.

In the case of cubic equations it is evident that each root is not necessarily a rational function of every other one since two of these roots may be complex and the third real. It is, however, easy to construct special irreducible cubic equations which have the property that each root is a rational function of some one, and hence to find numbers which generate a normal domain belonging to the group of order 3. To find one such number we may consider the imaginary seventh roots of unity  $\theta, \theta^2, \theta^3, \theta^4, \theta^5, \theta^6$ . We shall thus find also a domain belonging to the cyclic group of order 6.

In fact, if we replace  $\theta$  successively by  $\theta, \theta^2, \dots, \theta^6$  in the following equations:

$$\rho_1 = \theta, \quad \rho_2 = \theta^2, \quad \rho_3 = \theta^3, \quad \rho_4 = \theta^4, \quad \rho_5 = \theta^5, \quad \rho_6 = \theta^6$$

we evidently obtain the group of the totitives mod 7, and this is the cyclic group of order 6.\* It therefore results that the number  $\theta$  generates a domain which belongs to the cyclic group of order 6. Since  $\rho_1, \rho_6; \rho_2, \rho_5; \rho_3, \rho_4$  are the three systems of imprimitivity of this cyclic group, corresponding to its subgroup of order 2, it results that *each of the three numbers*

$$\psi_1 = \theta + \theta^6, \quad \psi_2 = \theta^2 + \theta^5, \quad \psi_3 = \theta^3 + \theta^4$$

*generates a domain of rationality which belongs to the group of order 3.*

To verify this statement we may observe that these three numbers are the roots of the irreducible equation  $x^3 + x^2 - 2x + 1 = 0$ , and that

$$\begin{aligned} \psi_1 &= \varphi_1(\psi_1) = \psi_1, & \psi_2 &= \varphi_2(\psi_1) = \psi_1^2 - 2, & \psi_3 &= \varphi_3(\psi_1) = -\psi_1^2 - \psi_1 + 1, \\ \psi_2 &= \varphi_1(\psi_2) = \psi_2, & \psi_3 &= \varphi_2(\psi_2) = \psi_2^2 - 2, & \psi_1 &= \varphi_3(\psi_2) = -\psi_2^2 - \psi_2 + 1, \\ \psi_3 &= \varphi_1(\psi_3) = \psi_3, & \psi_1 &= \varphi_2(\psi_3) = \psi_3^2 - 2, & \psi_2 &= \varphi_3(\psi_3) = -\psi_3^2 - \psi_3 + 1. \end{aligned}$$

Since the given cyclic group of order 6 has for its two systems of imprimitivity, corresponding to its subgroup of order 3, the two sets  $\rho_1, \rho_2, \rho_4; \rho_3, \rho_5, \rho_6$ , it results that each of the two numbers  $\theta + \theta^2 + \theta^4, \theta^3 + \theta^5 + \theta^6$  generates a domain which belongs to the group of order 2. In fact, these numbers are the roots of the irreducible equation  $x^2 + x + 2 = 0$ .

We proceed to determine a domain for each of the two groups of order 4. If  $\alpha$  is an imaginary fifth root of unity it satisfies the irreducible equation  $x^4 + x^3 + x^2 + x + 1 = 0$ , and the other three roots of this equation are  $\alpha^2, \alpha^3, \alpha^4$ . Hence the group of the domain generated by  $\alpha$  is the group of the totitives mod 5; that is, the group of the four numbers 1, 2, 3, 4 when these numbers are multiplied together and the products are reduced mod 5.

\* Cf. P. Bachmann, *Die Elemente der Zahlentheorie*, 1892, p. 89.

It is easy to verify, and well known, that this group is the cyclic group of order 5, and hence *each complex fifth root of unity generates a domain belonging to the cyclic group of order 4.*

As an instance of a domain which belongs to the non-cyclic group of order 4 we may mention the one which is generated by  $\rho_1 = p_1^{\frac{1}{2}} + p_2^{\frac{1}{2}}$ , where  $p_1$  and  $p_2$  are distinct rational prime numbers. It is easy to verify that  $\rho_1$  is a root of the irreducible equation

$$x^4 - 2(p_1 + p_2)x^2 + (p_1 - p_2)^2 = 0.$$

Adopting the notation

$$\begin{aligned}\rho_1 &= p_1^{\frac{1}{2}} + p_2^{\frac{1}{2}}, & \rho_3 &= -p_1^{\frac{1}{2}} + p_2^{\frac{1}{2}}, \\ \rho_2 &= p_1^{\frac{1}{2}} - p_2^{\frac{1}{2}}, & \rho_4 &= -p_1^{\frac{1}{2}} - p_2^{\frac{1}{2}},\end{aligned}$$

it is clear that the first three powers of  $\rho_1$  give rise to only three linearly independent irrational numbers in the natural domain; viz.,  $p_1^{\frac{1}{2}}$ ,  $p_2^{\frac{1}{2}}$ , and  $p_1^{\frac{1}{2}}p_2^{\frac{1}{2}}$ . The determinant of the system of the three equations thus formed cannot vanish since there is no rational relation between these powers of  $\rho_1$  because  $\rho_1$  is a root of an irreducible equation of degree 4. Hence these equations can be solved and each of the roots  $\rho_1$ ,  $\rho_2$ ,  $\rho_3$ ,  $\rho_4$  can be expressed as a rational function of any one of them.

It is now easy to see that the group of the domain generated by  $\rho_1$  is actually the non-cyclic group of order 4. In fact, all the substitutions besides the identity of this domain must involve a transposition, since these roots consist of two components, which are linearly independent in the natural domain, and these components differ only with respect to sign. Hence we pass from one of these roots to the other, in the functions which express all of them in terms of a particular one, by means of an operation of period 2. These observations may easily be verified by actually computing the functions in question and then replacing  $\rho_1$  by each of the other roots. The functions are as follows:

$$\begin{aligned}\rho_1 &= \varphi_1(\rho_1) = p_1^{\frac{1}{2}} + p_2^{\frac{1}{2}} = \rho_1, \\ \rho_2 &= \varphi_2(\rho_1) = p_1^{\frac{1}{2}} - p_2^{\frac{1}{2}} = \frac{\rho_1^3 - 2(p_1 + p_2)\rho_1}{p_2 - p_1}, \\ \rho_3 &= \varphi_3(\rho_1) = -p_1^{\frac{1}{2}} + p_2^{\frac{1}{2}} = \frac{\rho_1^3 - 2(p_1 + p_2)\rho_1}{p_1 - p_2}, \\ \rho_4 &= \varphi_4(\rho_1) = -p_1^{\frac{1}{2}} - p_2^{\frac{1}{2}} = -\rho_1.\end{aligned}$$

If  $\rho_1$  is replaced successively by  $\rho_1$ ,  $\rho_2$ ,  $\rho_3$ ,  $\rho_4$ , there result the substitutions of the four group; that is, *the number  $p_1^{\frac{1}{2}} + p_2^{\frac{1}{2}}$ , where  $p_1$  and  $p_2$  are distinct rational prime numbers, generates a domain whose group is the non-cyclic group of order 4.*

To find a domain belonging to the group of order 5 we may use the ten complex eleventh roots of unity. Each of these roots generates a domain belonging to the cyclic group of order 10 and the pairs of roots corresponding to the five systems of imprimitivity of this cyclic group must therefore generate a domain belonging to the group of order 5. If these ten complex roots are  $\beta, \beta^2, \beta^3, \beta^4, \beta^5, \beta^6, \beta^7, \beta^8, \beta^9, \beta^{10}$ , the group of the domain generated by  $\beta$  involves the following substitution:

$$(\beta\beta^2\beta^4\beta^8\beta^5\beta^{10}\beta^9\beta^7\beta^3\beta^6).$$

Hence each of the five numbers

$$\beta + \beta^{10}, \quad \beta^2 + \beta^9, \quad \beta^3 + \beta^8, \quad \beta^4 + \beta^7, \quad \beta^5 + \beta^6$$

generates a domain belonging to the group of order 5. It is not difficult to prove that the irreducible equation which has these five numbers as roots is as follows:

$$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1.$$

The domains which have been considered thus far are called *abelian* since they belong to an abelian group. We proceed now to determine a non-abelian domain; viz., one which belongs to the symmetric group of order 6. The domain generated by  $\rho_1 = \sqrt{-3} + p^{\frac{1}{2}}$ ,  $p$  being any prime number, is non-abelian. In fact, the six roots of the irreducible equation which is satisfied by  $\rho_1$  are as follows:

$$\begin{aligned} \rho_1 &= \sqrt{-3} + p^{\frac{1}{2}}, & \rho_2 &= \sqrt{-3} + \omega p^{\frac{1}{2}}, & \rho_3 &= \sqrt{-3} + \omega^2 p^{\frac{1}{2}}, \\ \rho_4 &= -\sqrt{-3} + p^{\frac{1}{2}}, & \rho_5 &= -\sqrt{-3} + \omega p^{\frac{1}{2}}, & \rho_6 &= -\sqrt{-3} + \omega^2 p^{\frac{1}{2}}. \end{aligned}$$

The substitution which corresponds to the case when  $\rho_1$  is replaced by  $\rho_4$  merely changes the sign of  $\sqrt{-3}$ , and hence it is as follows:  $(\rho_1\rho_4)(\rho_2\rho_6)(\rho_3\rho_5)$ . The substitution corresponding to the case when  $\rho_2$  is replaced by  $\rho_5$  changes the sign of  $\sqrt{-3}$  and multiplies  $p^{\frac{1}{2}}$  by  $\omega^2$ . Hence it is as follows:  $(\rho_1\rho_6)(\rho_2\rho_5)(\rho_3\rho_4)$ . As these two substitutions of order 2 have a product of order 3 they generate the dihedral group of order  $6^*$ , which is simply isomorphic with the symmetric group of order 6. This proves the following theorem: *the number  $\sqrt{-3} + p^{\frac{1}{2}}$  generates a domain which belongs to the symmetric group of order 6.*

It remains only to construct a domain belonging to the group of order 7. This may readily be done by means of the complex roots of the equation  $x^{29} - 1 = 0$ . If  $\theta$  is such a complex root it generates a domain which belongs to the cyclic group of order 28. Each of the seven distinct sets of sums of four roots corresponding to the subgroup of order 4 in this cyclic group of

\* G. A. Miller, Bulletin of the American Mathematical Society, vol. 7 (1901), p. 424.

order 28 must therefore generate a domain which belongs to the group of order 7. As 12 belongs to exponent 4 mod 29, it results that one of these seven sets of numbers is  $\theta + \theta^{12} + \theta^{28} + \theta^{17}$ . That is, *if  $\theta$  is a complex root of the equation  $x^{29} - 1 = 0$  then will the number  $\theta + \theta^{12} + \theta^{28} + \theta^{17}$  generate a domain which belongs to the group of order 7.*

## 2. Domains Belonging to Two Infinite Systems of Groups.

One of the most elementary infinite categories of groups is composed of all the possible groups which involve only operators of order 2, in addition to the identity. There is one and only one such group of order  $2^m$ ,  $m$  being an arbitrary positive rational integer, and all of these groups are abelian.\* It is very easy to find a domain of rationality for each one of these groups. In fact, the number  $\rho_1 = p_1^{\frac{1}{2}} + p_2^{\frac{1}{2}} + \cdots + p_m^{\frac{1}{2}}$ , where  $p_1, p_2, \cdots, p_m$  are distinct rational prime numbers, generates a domain which belongs to this group of order  $2^m$ . To prove that each of the  $2^m$  numbers  $\pm p_1^{\frac{1}{2}} \pm p_2^{\frac{1}{2}} \pm \cdots \pm p_m^{\frac{1}{2}}$  is a rational function of  $\rho_1$  we observe that the first  $2^m - 1$  powers of  $\rho_1$  involve exactly  $2^m - 1$  irrational numbers such that no two of them have a rational ratio, since the number of linear combinations of  $p_1, p_2, \cdots, p_m$  is

$$m + \frac{m(m-1)}{2!} + \frac{m(m-1)(m-2)}{3!} + \cdots + m + 1 = (1+1)^m - 1 = 2^m - 1.$$

As  $\rho_1$  is a root of an irreducible equation of degree  $2^m$ , whose roots are  $\pm p_1^{\frac{1}{2}} \pm p_2^{\frac{1}{2}} \pm \cdots \pm p_m^{\frac{1}{2}}$ , it results that the given  $2^m - 1$  powers of  $\rho_1$  are linearly independent in the absolute domain of rationality. Hence the determinant of the system of  $2^m - 1$  equations arising from these powers, the unknowns being the  $2^m - 1$  combinations of  $p_1^{\frac{1}{2}}, p_2^{\frac{1}{2}}, \cdots, p_m^{\frac{1}{2}}$ , cannot vanish. That is, each of these unknowns is a rational function of  $\rho_1$ . In particular, each of the  $2^m$  numbers  $\pm p_1^{\frac{1}{2}} \pm p_2^{\frac{1}{2}} \pm \cdots \pm p_m^{\frac{1}{2}}$  is a rational function of  $\rho_1$ .

Suppose that each of these numbers is expressed rationally in terms of  $\rho_1$ . If we replace  $\rho_1$ , in each of these  $2^m$  functions, by its value  $p_1^{\frac{1}{2}} + p_2^{\frac{1}{2}} + \cdots + p_m^{\frac{1}{2}}$ , the coefficients of each of the  $2^m - 1$  given unknowns, except those of  $p_1^{\frac{1}{2}}, p_2^{\frac{1}{2}}, \cdots, p_m^{\frac{1}{2}}$ , must vanish. If we replace  $\rho_1$  by any other one of the roots  $\pm p_1^{\frac{1}{2}} \pm p_2^{\frac{1}{2}} \pm \cdots \pm p_m^{\frac{1}{2}}$  in each of these  $2^m$  functions, the same coefficients must evidently vanish, and the values of these functions can be obtained from those in which the value of  $\rho_1$  was substituted by merely effecting the corresponding changes of signs in the coefficients of  $p_1^{\frac{1}{2}}, p_2^{\frac{1}{2}}, \cdots, p_m^{\frac{1}{2}}$ . As this is an operation of period two, it results that all the non-identical substitutions of the domain generated by  $\rho_1$  must involve cycles of order 2.

\* G. A. Miller, Quarterly Journal of Mathematics, vol. 28 (1896), p. 208.

As these substitutions are also regular, it follows that they all are of order 2, That is, *the domain of rationality generated by the number  $p_1^{\frac{1}{2}} + p_2^{\frac{1}{2}} + \dots + p_m^{\frac{1}{2}}$ , where  $p_1, p_2, \dots, p_m$  are distinct rational prime numbers, belongs to the abelian group of order  $2^m$  and of type  $(1, 1, 1, \dots)$ .*

Another very elementary infinite system of abelian groups is composed of all the groups which can be represented as groups of totitives; that is, all the groups formed by the  $\varphi(m)$  positive rational integers which do not exceed  $m$  and are prime to  $m$  when these integers are combined by multiplication and the products are replaced by their least positive residues mod  $m$ ,  $m$  being an arbitrary positive rational integer. This infinite category of groups may also be defined as composed of the groups of isomorphisms of all possible cyclic groups.

It is well known that the equation of degree  $\varphi(m)$ , whose roots are the  $\varphi(m)$  primitive roots of the equation  $x^m = 1$ , is irreducible.\* If  $\theta$  represents one of these roots each of the other roots may be obtained by raising  $\theta$  to the powers whose indices are the  $\varphi(m)$  totitives of  $m$ . Hence it results that these roots are permuted according to this group of totitives if we express all of them in terms of  $\theta$  and then replace  $\theta$  in these expressions successively by each one of them. In other words, *any primitive  $m$ th root of unity generates a domain whose group is the group of the totitives of  $m$ .*

While it is thus easy to find a domain of rationality whose group is an arbitrary group of totitives, and to construct a domain for each one of a very interesting system of abelian groups, the most important matter related to this subject has not yet been mentioned. This may be stated as follows: *It is possible to find a group of totitives which has any arbitrary abelian group as one of its quotient groups.* Since a transitive abelian group permutes a set of systems of imprimitivity according to each one of its possible quotient groups, it results from the italicized theorem which has just been stated that *it is always possible to find sums of primitive roots of unity such that each of these sums generates a domain of rationality belonging to any arbitrary selected abelian group.* We proceed to establish these theorems.

To prove the former of these two theorems we need only combine the following two well known results: Every arithmetic progression in which the first term and the common difference are relatively prime involves an infinite number of prime numbers, and an abelian group has a quotient whose invariants are the same as the invariants of any given subgroup of this abelian group. From the former of these two theorems it results that there is an infinite number of different primes such that each of them diminished by unity is divisible by an arbitrary number  $n$ , and hence it is possible to find a number  $m$  such that the group of totitives involves an arbitrary number

\* Cf. P. Bachmann, Die Lehre von der Kreisteilung, 1872, p. 321.

of independent cyclic subgroups of order  $n$ ,  $n$  being an arbitrary positive rational integer. Hence it results from the latter of the given theorems that it is possible to find a group of totitives whose quotient group has an arbitrary set of positive rational integers as invariants.

If an abelian group is represented as a transitive substitution it must be regular and it must involve systems of imprimitivity corresponding to each one of its subgroups. In the group of totitives under consideration we can therefore add the roots which belong to the same system of imprimitivity and thus obtain a number which has the same number of conjugates as the order of the quotient group which corresponds to the subgroup under consideration. This general method was illustrated in the preceding section when domains of rationality belonging to the group of orders 5 and 7 were determined. From what precedes it results that this method can be used to construct a domain belonging to any given abelian group, as was stated above. In particular, we can also construct by this method a domain belonging to any one of the infinite systems of abelian groups of order  $2^m$  and of type  $(1, 1, 1, \dots)$ , which were considered above.

The proof of the theorem that every possible abelian group is contained in some group of isomorphisms of a cyclic group directs attention to the question whether every possible non-abelian group is contained in a group of isomorphisms of some non-cyclic abelian group. That this question can be answered in the affirmative is evident from the fact that in an abelian group of order  $p^m$  and of type  $(1, 1, 1, \dots)$  we can establish an isomorphism in which a particular set of independent generators corresponds to itself as a whole but permutes these generators according to an arbitrary substitution of degree  $m$ .

Hence it follows that the group of isomorphisms of this abelian group contains as a subgroup a group which is simply isomorphic with the symmetric group of degree  $m$ . As every possible group is simply isomorphic with some subgroup of a symmetric group, we have established, as a special case, the theorem that *every possible group is isomorphic with a subgroup in the group of isomorphisms of an abelian group.*

---